M-grid User Security Guide

Introduction

This document is intended to cover security related aspects of M-grid from the user's perspective. It advises the user about security practices, individual user responsibilities and implications of using the grid.

Users must read and comply with the M-grid Acceptable Use Policy.

Logging in

- Remember: Your account is personal and may not be shared with other people.
- You can login to your own account on your local M-grid frontend with ssh.
- You should login to your local M-grid frontend only from a computer you trust. Other computers may have keyloggers installed and your password may be compromised.
- Protect all your keys with a passphrase.
- When possible, login using keys as it is more secure than using passwords.
- These instructions also apply when using alternate login interfaces, e.g. web portals.

Managing passwords, keys and certificates

- Remember to always use a good password or passphrase. A good password and passphrase must be very difficult for others to guess, they have at least 8 characters consisting of both upper and lower case letters, numbers and symbols and it must not be stored in an unencrypted file.
  - For more information about passphrases see the Wikipedia definition of a passphrase
- Keys are your identity - store your keys securely somewhere where only you have access.
- If you use ssh keys, they should be protected with a good passphrase. Unprotected ssh-keys are a significant security risk. SSH-Agent makes key usage easier and even more secure. For more information see http://wiki.hip.fi/twiki/bin/view/Extranet.MGrid/Extranet.MGrid.SSHAgentGuide
- Ensure that your grid key is protected by a good passphrase and not viewable by other users
- Your key is stored on the machine from which you apply for a certificate. Apply for certificates only from trusted machines.
- Never share your passwords, certificates or keys with other users - even with administrators

Running grid jobs

- Only submit grid jobs from a computer you trust.
- Grid jobs are submitted using proxy certificates which you create with your grid certificate. Your proxy certificate is your identity and is transferred to the cluster on which your job is executed. It is not protected by a password therefore it should not be valid for longer than necessary for the job to complete. Proxy certificates can be easily renewed.

Privacy and user data

- M-grid is not designed for storing or transmitting sensitive data.
- While data transfers are securely authenticated, the data transfer itself is not encrypted for performance reasons.
- Some information about jobs submitted locally via the batch queue system is available to other users logged in to that cluster.
- Some information about jobs submitted via the grid interface is available publically via the Grid Information system. This includes, but is not restricted to, your name, job description and submission host.
- Contact and usage information for M-grid users is kept by local M-grid administrators and may be shared between M-grid partners for administrative purposes.

Security incidents

- If you suspect that your account, password, pasphrase, key or certificate has been compromised, you must advise the local M-grid administrator as soon as possible. If the local administrator is not available, M-grid administrators at CSC should be advised.
- You must immediately report any suspected misuse of grid resources to the M-grid administrators.
- Contact information for M-grid administrators can be found here: http://www.csc.fi/english/research/Computing_services/mgrid/data_security_and_privacy/index_html

Related documents:

- M-grid Acceptable Use Policy (Compulsory reading for M-grid users)
- M-grid Security Policy
- Security Guide For Administrators

This topic: Extranet/MGrid/SecurityWG > SecurityGuideForUsers
History: r37 - 23 Feb 2009 - 12:52:10 - MichaelGindonis